eSafety Commissioner - Senate Estimates, October 2025: Opening statement

Thank you for the opportunity to provide an update on a very busy period since the last hearing in February, including the recent proliferation of extreme violent material we've seen online.

Unfortunately, this is not the first time I have addressed the committee on this topic. I again note the potential of such material to normalise, desensitise and sometimes radicalise young Australians, as highlighted by ASIO director General Mike Burgess.

Terrorist and violent extremist material used to make up a tiny fraction of complaints to eSafety– around 3% – but we've seen a 55% increase so far this financial year.

Last month, my teams spent an inordinate amount of time and energy investigating videos extensively posted and shared over a short period of time, making them widely accessible to Australian users including children.

They captured three tragic events in the United States in graphic detail: the assassination of Charlie Kirk, the horrific murder of Ukrainian student Iryna Zarutksa, and the decapitation of a hotel manager in Dallas.

I know many Australian parents were disturbed to discover close-range footage of the Charlie Kirk shooting in particular appearing without warning in the social media feeds of their children.

eSafety sought urgent review by the Classification Board, which assessed instances of material showing all three attacks as Refused Classification (RC).

We then engaged with major technology companies to inform them of their obligations in relation to such material, issuing removal notices in some instances where they were not complying.

This week we issued an Online Safety Advisory to help parents and educators deal with the potential impact of material known collectively as 'gore', which our research shows has now been viewed by 22 per cent of Australian children between the ages of10 and 17.

We're also addressing children's exposure to high-impact, age-inappropriate content at a systemic level through the implementation of codes and standards drafted by industry and registered by me in September.

These newer codes create significant additional obligations for online services to prevent children's exposure to extreme violence, pornography, suicidal ideation, self-harm material and the outputs of sexualised AI-driven chatbots.

The codes will provide another layer of protection for under-16s on services that are not age restricted when social media minimum age obligations come into force on December 10.

I know the Social Media Minimum Age is a topic that will interest the committee greatly, and I'm pleased to be able to say we have made significant progress towards implementing it.

We have undertaken broad consultation with over 160 organisations and 345 individuals across industry, community organisations, educators, parents and young people.

That process helped inform our regulatory guidance for industry, which has been well-received as reasonable, feasible and fair.

To further support industry, we released a self-assessment tool to assist services in determining whether they will be subject to the SMMA obligations – with the understanding they need to seek their own legal advice.

In July the Government indicated its view that the following platforms would be age-restricted on December 10:

- YouTube
- Facebook
- Instagram
- TikTok
- X, and
- Snapchat

We have been engaging with platforms and conducting our own assessments and I can confirm to the committee today that, based on our preliminary assessments, eSafety agrees with that view.

Whilst some platforms have already indicated they agree with our assessments, some services are likely to respond with their alternate view and may also provide additional information that may change our assessments.

We recognise the community needs information about exactly how the social media landscape will change after 10th December. Information will be available for parents, carers and the community in the lead into the law coming into effect, including comprehensive resources to help families and schools navigate this important change.

However, consistent with our advice to Minister Wells earlier in the year, we will take a dynamic approach. Technology is constantly evolving and I don't believe there can ever be a static list of "who's in and who's out".

New potential social media services may appear without warning, as we saw last week with OpenAI's release of AI-generated social app "Sora", and existing services change.

eSafety expects services to continue to review their self-assessments as they add new features and functions, or as their user engagement patterns shift.

In terms of compliance and enforcement, we'll be taking a risk and outcomes-based approach, focusing on platforms with the highest number of young Australian users.

We have already been engaging with platforms regarding our expectations come 10 December and we'll use a variety of tools and strategies, including our information gathering powers to source relevant data.

Importantly, we will be focusing on systemic compliance failures, rather instances of individual underage accounts.

The regulatory developments I've described today comprise only a part of our recent activity, including enforcement action to protect children against grooming and the scourge of sexually explicit deepfakes tearing apart our schools and communities.

They highlight eSafety's transition from a reactive, complaints-based model, to a more systemic one, providing a comprehensive protection for all Australians.

Today, we exercise powers to mandate critical public transparency and enforce systemic non-compliance with the rules of the road across the technology industry.

This is the model is clearly prescribed in the Online Safety Act.

One thing I can say with certainty is that the harms Parliament set out to address when it passed the Act in 2021 have not diminished.

On the contrary, they have only grown.

I am happy to take questions from the committee on this and any other issues you wish to raise.

Thank you.